Version 2.0 May 2020

China CITIC Bank
London Branch

Outsourcing Policy

中信银行 CHINA CITIC BANK 伦敦分行 LONDON BRANCH

Document History

Owner	Chief Risk Officer	**Status**	Approved
Version	2.0	**Date**	May 2020
Approved by	Management Committee		
Approved Date	22/5/2020	**Next Review Date**	March 2021
Location	London		

Version	Owner	Approval	Date	Major changes
1.0	President	President	May 2018	PRA Regulatory Business Plan
1.1	CRO	MANCO	Oct 2018	As per ManCo approval dated October 18
2.0	CRO	MANCO	May 2020	• Risk assessment – add 'Anti-Bribery /Corruption' requirement, page 16 • Appendix A – Process, Management oversight – changed to CRO, page 24 • Appendix D – add Outsourcing contract check list, page 30

Contents

1 Introduction

This document forms the Outsourcing Policy of China CITIC Bank London Branch ("the Branch" and/or "CNCBLB") and sets out the approach the Branch takes to manage its outsourced activities.

This document aims to capture the respective roles, responsibilities and requirements of the Branch where activities and/or processes are outsourced to any third party.

The Branch will exercise due skill, care and diligence when entering into, managing, or terminating any critical outsourced arrangements in place with the respective service providers.

2 Policy Objectives

The Branch and its employees are obliged to behave in a way that supports the confidentiality, integrity and continuity of the Branch's business activities. Consequently, outsourced functions that do not apply the requirements of Chapter 8 of the Senior Management, Systems and Controls ("SYSC") must be documented and authorised by the Management Committee ("ManCo").
This policy is designed to ensure the Branch's outsourcing arrangements are compliant with SYSC 8. The extent to which compliance with this policy and SYSC 8 are achieved will also be reviewed as part of the Compliance Monitoring Programme ("CMP"). This policy covers matters relating to material outsourcing relationships, as defined in Section 5.

The objectives of this policy are to:

- Ensure that outsourcing is undertaken in a manner that does not lead to undue operational risks and does not impair the quality of internal controls or services provided to customers;

- Ensure that the requirements of the PRA and FCA are met at all times, including but not limited to the regulators' ongoing ability to supervise and monitor the Bank's compliance with regulatory obligations; and
- Set out the outsourcing process for material outsourcing arrangements and associated requirements, roles and responsibilities.

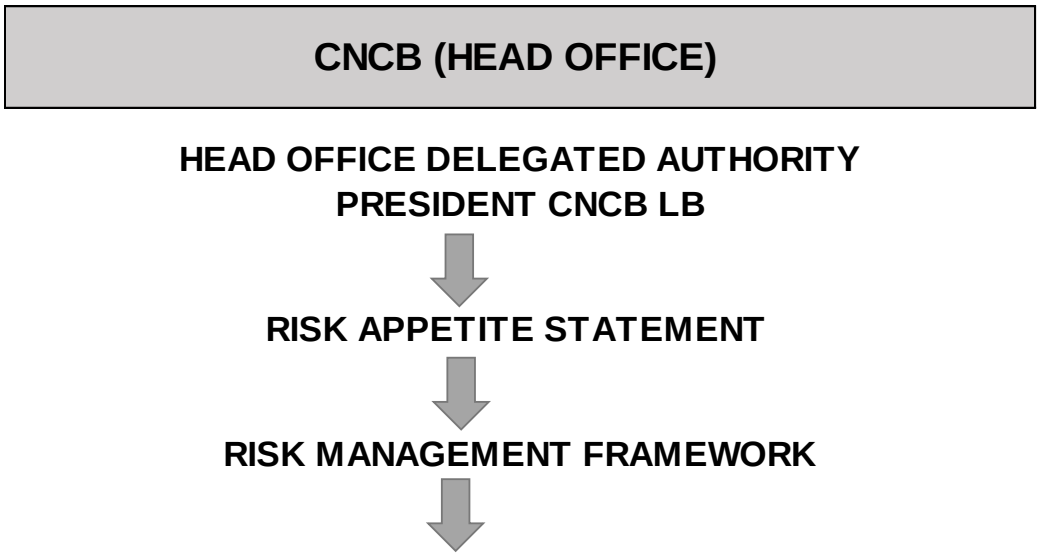
3 Policy Ownership

The 'ownership chain' for the Policy is set out below:

Document Owner	The Branch's Chief Risk Officer ("CRO") is responsible for the maintenance of this document. The CRO will also be responsible for reviewing the ongoing adequacy of the policy on an annual basis or as required. Any material changes to this document will be subject to the approval of ManCo and communicated to appropriate staff accordingly.
Challenge and oversight	The Audit and Risk Committee ("ARCo") will review and challenge this policy and its subsequent framework at least annually or more frequently as necessary. If an issue arising from this policy presents a material risk to the Branch or one of its customers then the Chief Compliance Officer ("CCO") will escalate the matter to the ARCo, or the regulators as appropriate.
Approval	The ManCo, based on a recommendation from ARCo is responsible for the approval of this document following each review by ARCo.
Applicability	All members of staff, whether permanent (local hires and Expatriate alike) or contractors must operate in accordance with this Policy. Escalation of any matters arising in respect of this policy should be via the individual's Head of Department or directly to the CRO. To ensure compliance with the requirements of this policy the CCO will also conduct ad-hoc reviews as per the Branch's CMP.

4 Governance & Risk Management Framework

The Outsourcing Policy is a supporting policy for the Operational Risk framework that is integral part of the overall risk framework, which is presented as follows:



RISK	PRIMARY RISK MANAGEMENT FRAMEWORK
CREDIT RISK	Credit Approval and Credit Risk Management Policy
MARKET RISK	Market Risk Management Policy
OPERATIONAL RISK	Operational Risk Management Policy Outsourcing Policy Business Continuity Management Framework New Products Approval Policy Conduct Risk Policy Framework
LIQUIDITY RISK	Liquidity Risk Management Policy

Risk department will manage the outsourcing and third-party supplier through the outsourcing process requirements, critical outsourcing monitoring, supplier risk assessment and review.

5 Roles and Responsibilities

A summary of the roles and responsibilities at various levels with respect to outsourced activities are detailed below:

Role/Committee	Function
ManCo	Decides whether a particular service will be outsourced as opposed to being performed in-house and determines whether it is a material outsourcing relationship. ManCo will review the business case based on recommendations from ARCo before making the final decision.
ARCo (Challenge and Recommendation)	The ARCo will review the decision on the vendor/supplier selection process and submit to ManCo for approval. The ARCo will review the business case and vendor/supplier selection particulars provided by the Head of Department and submit its decision to ManCo for approval. ARCo is responsible for the annual review of this policy. The ARCo will also serve as the escalation point for crystallised issues regarding outsourced providers.
Heads of Department (Proposer and Responsible for individual relationships post appointment)	Heads of Department will assess the business need for Outsourcing of permissible financial and other services as and when they require taking into consideration the commercial aspects of the decision. They must develop the business case and present the case to ARCo. Heads of Department will provide reports to ARCo on the appropriateness of vendors/suppliers during the selection process and indicate its preferred supplier. They will also be responsible for carrying out due diligence at the time of selection process and subsequent renewals of outsourced activities with the support of the Risk Management and Compliance departments as necessary.
Second Line of Defence	The Risk department will be responsible for keeping a record of all outsourced services and ensuring that they are correctly categorised.

	Both the Risk and the Compliance Departments play an active role in both the vendor/supplier selection process and due diligence and will provide advice and recommendations where appropriate on the suitability of the vendor/supplier, taking into consideration all material risks, including the vendor/supplier's control environment.
Operations	The Head of Operations will be responsible for back office operations and for payments services (including the individual relationship with the clearing bank to be appointed).
IT	The Head of IT will have day to day oversight of all the IT outsourcing arrangements that the Branch will have with HO.
Internal Audit	The outsourced Internal Audit function will periodically review the nature of outsourcing arrangements as per its annual audit plan to ensure they are compliant with regulatory rules and guidance and ongoing monitoring is in line with the standards set out in this policy. The Internal Audit function will also review the internal process to outsource services to ensure compliance with regulatory rules and guidance. The reports, reviews and findings will be provided to the ARCo.

6 Regulatory and Legal Requirements

6.1 UK Systems & Controls

As a core principle for all outsourcing arrangements entered into, CNCBLB will outsource functions and services only insofar as this can be done in a manner that does not impair the adequacy of internal controls; or the service provided to customers.

Furthermore, this policy will also ensure that the requirements of the Prudential Regulatory Authority ("PRA") and Financial Conduct Authority ("FCA") are met at all times including but not

limited to the regulators' ongoing ability to supervise and monitor the Branch's compliance with regulatory obligations. In particular, the FCA sets out requirements and guidance in respect of Outsourced functions and services within Chapter 8 of SYSC.

With regard to SYSC 8, those interacting with the outsourcing process must also bear in mind the following guidelines:

- The Branch must complete appropriate level of due diligence checks on the nominated service provider;
- The service provider must have the ability, capacity, and any authorisation required by law to perform the outsourced functions, services or activities reliably and professionally;
- The service provider must properly supervise the carrying out of the outsourced functions, and adequately manage the risks associated with the outsourcing;
- Appropriate action must be taken if the service provider is not carrying out their functions effectively and in compliance with applicable laws and regulatory requirements and/or is breaching the terms and conditions of the contractual arrangements entered into (including any Service Level Agreements ("SLAs")) between both parties;
- The Branch must retain the necessary expertise to supervise the outsourced functions effectively and manage the risks associated with the outsourcing;
- The service provider must disclose to the Branch any development that may have a material impact on its ability to carry out the outsourced functions effectively and in compliance with applicable laws and regulatory requirements;
- The Branch must be able to terminate the arrangement for the outsourcing where necessary without detriment to the continuity and quality of its provision of services to clients;

- The Branch and its regulators authority must have access to data related to the outsourced activities; and
- The Branch must ensure that the relationships and the obligations towards its customers must not be altered or affected by the outsourcing arrangements.

6.2 Other Laws and Regulations

- **UK Data Protection Bill (European GDPR)**, the Data Protection Bill (DPB) was released on 13 September 2017and the bill is designed to bring the UK's data protection laws in line with the European Union's ("EU") General Data Protection Regulation ("GDPR"). The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established. Although the key principles of data privacy still hold true to the previous directive; the key points of the GDPR are highlighted below:

  - Increased Territorial Scope (extra-territorial applicability) -the regulatory landscape of data privacy has extended jurisdiction, as it applies to all companies processing the personal data of data subjects residing in the European Union, regardless of the company's location.
  - Penalties - any breach can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements. It is important to note that these rules apply to both controllers and processors, meaning 'clouds' will not be exempt from GDPR enforcement.
  - Consent - must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

- Data Subject Rights - *Breach Notification*, mandatory where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. *Right to Access*, part of the expanded rights of data subjects is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. *Right to be Forgotten*, also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. *Data Portability*, the right for a data subject to receive the personal data concerning them, which they have previously provided in a '*commonly use and machine-readable format*' and have the right to transmit that data to another controller.

- **Cloud Service Providers**, FCA GC 15/6 guidance for firms outsourcing to the 'cloud' and other third-party IT Services notes that in addition to current risk assessments, the following five key areas should be considered for cloud-based service providers:

1. **Proportionality and Materiality Assessment,** where the outsourcing is assessed as material, the financial institution must notify its regulator before that outsourcing can take place. The materiality assessment should cover:
    a. criticality and inherent risk profile of the activities to be outsourced;
    b. complexity of the financial institution's activities;
    c. size, structure and operational environment of the financial institutions; and
    d. the potential impact of a confidentiality breach on the institution and its customers.

2. **Access and Audit Rights,** ensure an equivalent level of access to data as if the activity had not been outsourced by the financial institution. Access rights to the cloud service provider's business premises. The premises access rights also include a right to access all devices, systems, networks and data used for providing the outsourced services.
3. **Data Protection Controls,** *o*utsourcing institutions are expected to ensure adequate systems and controls to protect the confidentiality, integrity and availability of data when it is being processed, transferred and stored. Additional risk assessments, such as the political and security stability must be undertaken for cloud service outside the EEA.
4. **Chain outsourcing,** this potential risk arises where the outsourcing service provider sub-contracts some or all of the elements of the service to other providers. The outsourcing institution must retain the right to terminate a contract where the cloud service provider plans to change subcontractor or the sub-contracted services in a way which would have an 'adverse effect' on the risk assessment of the agreed services.
5. **Termination and exit management,** contingency planning and exit strategies for cloud outsourcing should include termination and exit management clauses. These clauses would allow the transfer of the outsourced activities to an alternative service provider or to be taken back in-house by the outsourcing institution.

The Modern Slavery Act 2015, applies to both public and private companies and partnerships, regardless of which sector they operate in and whether or not they were incorporated in the UK. These companies are required to comply with the provisions of the Act if they have a global net turnover of over £36 million and the company carries on business, or any part of their business, in the UK.

Companies who meet these criteria have an obligation to publish a “slavery and human trafficking statement” every year six months after the end of the company’s financial year. In accordance with section 53 of the Act 2015, the statement either outlines the steps that the company has taken during the financial year to ensure that slavery and human trafficking is not taking place within its supply chains or any part of their business.

As regards publication of the statement, if the organisations have a website the Act requires the company to publish it statement on the website and include a link to the document in a “prominent place” on that website. Companies without websites are required to provide a copy of the statement to anyone who makes a written request for it within 30 days of receiving the request.

7 Defining and Identifying Critical Outsourcing Relationships

CNCBLB define outsourcing as the Branches use of a supplier to perform activities that would normally be undertaken by CNCBLB itself”.

7.1 Definition of Critical

For an outsourcing relationship to be deemed ‘Critical’, it would have to involve outsourcing activities of such importance that any weakness or failure in the provision of these activities could have a significant effect on the Branch’s ability to meet its regulatory responsibilities.

7.2 Determining Materiality

The Branch assesses the criticality an outsourced relationship based upon a risk assessment considering such factors as, but not limited to:

- The impact of outsourcing on the service(s) provided to customers;

- The impact of outsourcing on the ability and capacity of the Branch to comply with regulatory requirements, with particular reference to the Regulators criteria set out in SYSC 8 (where SYSC 8 is relevant to the outsourced activity a written assessment against SYSC 8 will be made and retained to provide an audit trail of the assessment);
- The regulatory status of the service provider (i.e. whether the service provider is regulated and if so by which regulator);
- The impact of outsourcing on our operational controls;
- The financial, reputational and operational impact on the business of a failure of the service provider to perform;
- the regulatory status of the service provider;
- The financial status of the service provider; and
- The degree of difficulty and time required to select an alternative service provider or to bring the business activity in-house should the incumbent cease being able to perform services agreed.

Decisions and core management responsibility concerning strategic control may not be outsourced. Should a relationship be deemed Critical, it will be subject to the full monitoring programme as set out in the Branch's Outsourcing Policy. Where relying on HO or any other third-party for provision of an operational function or service, the Branch will take all reasonable steps to avoid operational risk outside of its risk appetite.

The ManCo will be responsible for determining whether the proposed outsourcing relationship is critical to the Branch, and whether an outsourcing contract is of a material nature based on a risk analysis of the service to be provided.

8 Risk Management

8.1 Risk assessment

The Branch will ensure that any outsourcing arrangement neither diminish its ability to fulfill its obligations to customers and regulators, nor impede effective supervision by regulators. Before entering into, or significantly changing, an outsourcing arrangement, CNCBLB will:

- analyse how the arrangement will fit within the organisation and reporting structure; business strategy; overall risk profile; and ability to meet its regulatory obligations;
- consider whether the agreements establishing the arrangement will allow it to monitor and control its operational risk exposure;
- conduct appropriate due diligence of the service provider's financial stability and expertise;
- conduct assessment on potential bribery and corruption of third-party service providers, this should cover a minimum of contract review, business partners code of conduct, training and any adverse news.
- consider how it will ensure a smooth transition of its operations from its current arrangements to a new or changed outsourcing arrangement (including what will happen on the termination of the contract); and
- consider any concentration risk implications such as the business continuity that may arise if a single service provider is used by several firms.
- Consider annual reviews and assessments of performance

ManCo retains overall accountable for the management, monitoring, reporting and control of risks arising from the business conducted by the Branch notwithstanding any outsourcing arrangements relied upon. Outsourcing does not result in the delegation of responsibility and will not affect the relationship and obligations of CNCBLB towards its clients and to the regulators.

On engaging with a service provider, the Branch undertakes a risk assessment exercise in conjunction with the prospective service provider. This assessment is used to identify the key risks associated with the proposed service(s) to be outsourced. The Branch is also required to develop, in partnership with the service provider, a system of controls designed, documented and implemented to manage the risks identified.

During the contracting process, the Branch is to undertake a risk assessment exercise in conjunction with the service provider, to identify key risks associated with the service(s) to be outsourced. The Branch and the service provider work together to ensure that a system of controls is designed, documented and implemented to manage the following risks identified.

The Risk and Compliance departments will be involved at all stages of the outsourcing process. The Risk and Compliance departments have the ability to veto any decisions in the outsourcing process where that decision would impact on the Branch's ability to comply with regulatory obligations.

Risk and Compliance will play an active role in both the vendor/supplier selection process. Should they feel that the service provider is not able to ensure that the services provided will allow threshold conditions to be met at all times. The Compliance function will also periodically review the monitoring of the performance of the services received.

Appendix A - Outsourcing process.

8.2 Contracts

The Branch will document the service arrangements through appropriate legally binding agreements.

All contracts for high-risk third-party supply activities shall be subject to documented annual reviews, in liaison with the relevant business area. All high-risk service contracts should, wherever possible, have performance management clauses that allow for the measurement of contractual performance against agreed service level standards.

All service arrangements must have an end date and/or a termination clause.

8.3 Potential Risks

CNCBLB is aware that it undertaking outsourcing activities (see ***Appendix B***) and using third-party vendor/suppliers (see ***Appendix C***) gives rise to several risks that need to be appropriately mitigated:

- **Business Strategy Risk –** the risk arising from erroneous business decisions, improper implementation of decisions or lack of responsiveness to industry changes. This risk is a function of the compatibility of organisation's strategic goals, the business strategies developed to achieve those goals, the resources deployed against these goals and the quality of implementation. The service provider may conduct business on its own behalf, which is inconsistent with overall strategic goals of the Branch.
- **Reputational Risk –** the risk arising from negative public opinion. The risk may expose the institution to litigation, financial loss or a decline in customer base. Poor service from the service provider and its customer interaction not being consistent with the overall standards of the Branch.

- **Legal and Compliance Risk –** The failure of a service provider in observing with UK legal and regulatory requirements can lead to levying of fines, penalties or punitive damages, resulting from supervisory actions. Additionally, risks arise arising from whether or not the Branch has the ability to enforce the contract.
- **Operational Risk –** This risk arises from failed or inadequate people, processes or systems in place which could include technology failure, fraud, errors, inadequate financial capacity to fulfil obligation and/or provide remedies.
- **Exit Strategy Risk –** This could arise from over reliance on one firm, the loss of relevant skills in the Branch itself preventing it from bringing the activity back in-house and contracts entered into wherein speedy exits would be prohibitively expensive
- **Concentration and Systemic Risk –** Due to lack of control of the Branch over a service provider or when the Branch or overall banking industry has considerable exposure to one service provider. Failure of a service provider in providing a specified service, a breach in security/confidentiality, or non-compliance with legal and regulatory requirements, among others may lead to reputation or financial losses for the Branch and may also result in systemic risks within the banking system in the country.

9 Record keeping requirements

The Branch will maintain all records pertaining to the outsourcing process in order to demonstrate compliance with relevant rules and regulations. The Branch policy is to retain this information for a minimum of 5 years after the end of the life cycle of the contract/termination of the contract.

Records will be maintained for the following:

- All correspondence documentation pertaining to the outsourcing arrangement, with the service provider and internally within CNCBLB;

- All supporting documentation used at the time of vendor/supplier selection;
- Documentation provided by the service provider to assess performance and compliance with SLAs;
- All financial information pertaining to the Branch-service provider relationship; and
- Any feedback received from any stakeholder (any individual involved in the outsourcing process).

Further details on record keeping can be found in CNCBLB Record Keeping Policy.

10 Review and Update of Policy

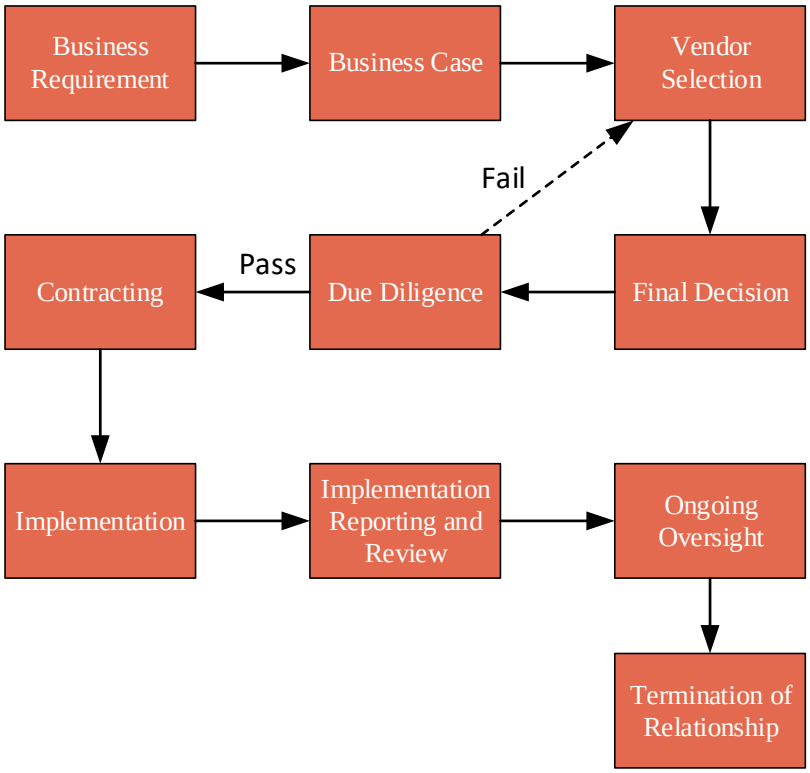
The Outsourcing Policy shall be reviewed by the Risk at least annually or as directed by the ManCo, to reflect changes in the profile of risks or business activities, organisational or authority structures or new regulations relevant to CNCB LB management of market risk.

11 Appendix A: Outsourcing Process

The Branch performs detailed due diligence of all service providers considered for the purposes of outsourcing (prior to selecting the service provider and before entering into the outsourcing arrangement). Each assessment should be supported by appropriate documentation, and the documentation should be stored both electronically and printed and filed.

The outsourcing process is shown in the diagram below.

CNCBLB Outsourcing Process



Business Requirement

The ManCo is responsible for a consensus decision that the business will outsource the provision of a particular service/process to an appropriate service provider, as opposed to being performed 'in-house'. The Head of the department wishing to outsource a particular service must develop a business case covering the areas set out in the next section.

Business Case

The department wishing to outsource a service will need to conduct a risk assessment and consider the following when submitting their proposal to ManCo:

- The level of importance to CNCBLB of the activity being outsourced;
- The potential impact of the outsourcing on the territory on various parameters such as earnings, solvency, liquidity, funding capital and risk profile;
- Precise details of the service/ process to be outsourced;
- The proposed life cycle of outsourcing;
- The likely impact on the Branch's reputation and brand value, and ability to achieve its business objectives, strategy and plans, impact on customer outcomes and service should the service provider fail to perform the service;
- The estimated prices and rates for the services over the lifetime of the contract;
- The costs associated with the ongoing relationship management; and
- The risks involved with the outsourcing of the service.

The budget for the proposed outsourcing arrangement must be approved by the ManCo prior to entering into a contract and associated SLA with the service provider.

The ManCo will review the business case, and where required, request amendments before giving approval or rejecting the application. Should approval be given, the relevant Head of Department will be invited to make a vendor/supplier selection.

Vendor/Supplier Selection

The Branch considers it best practice to invite at least three prospective providers to tender for the proposed service. However, the ManCo may decide that fewer providers should be selected depending on the nature of the service being outsourced. The ManCo will be responsible for reviewing information on the prospective providers and initiating the process of choosing the vendor/supplier best aligned to the Branch's goals. A report from the Head of Department will be provided to the ManCo, detailing how best potential supplier fulfils the business case.

Due Diligence

Due diligence will be carried out on the preferred service provider. The Head of Department wishing to outsource a service will be responsible for carrying out due diligence with support from the Risk and Compliance departments as necessary.

Due Diligence is performed using a risk based approach and documentation is required against the following criteria (as appropriate):

- Compliance with SYSC 8;
- Vendor/Supplier Risk Assessment;
- Financial Analysis and Review;
- Business Continuity Plans and/or testing results of Disaster Recovery plans;
- Review of SLAs;
- Results of Third-party information security assessments if Branch data is managed offsite; and
- Other information deemed appropriate based on the vendor/supplier and the associated level of risk.

If the service provider is allowed to sub-contract (which should remain exceptional), the same standards will have to be imposed on the sub-contractor.

If a vendor/supplier fails to pass the Branch's due diligence process, the outsourcing process will return to the selection phase for re-selection of a chosen service provider.

Final Decision

The relevant Head of Department will gather the relevant information including the business case, and vendor/supplier selection particulars (including preferred supplier) and submit this to the ARCo which will review and make any recommendations before being approval is provided by ManCo.

Contracting

The relationship between the relevant Head of Department and the service provider will be duly documented in a written and signed contract according to standards of the CNCBLB contract.

The legal requirements of each relevant jurisdiction will be considered before entering into the outsourcing contract. Special attention will be given to regulatory requirements concerning prior-notification/prior-approval.

Oversight

The outsourced service will be subject to oversight and internal management reporting by the relevant department. The second and third lines of defence (Compliance and IA respectively) are responsible for testing periodically, through the CMP, if monitoring by the relevant Head of Department adequate.

However, the primary risk oversight responsibility rests with the first line of defence and the Head of Department specifically.

Termination of Relationship

An outsourcing relationship could be terminated for several reasons, such as insufficient service being provided, superior service becoming available elsewhere, CNCBLB opting to bring the service back in-house or simply the outsourcing contract expiring.

The Branch will ensure the development of an exit plan in case the outsourcing arrangements are to be discontinued. This plan will, at the minimum:

- Describe the circumstances and the processes detailing how and when discontinuation may be pursued;
- List the timeframes involved;
- Detail the process of transfer of outsourced services back to the Branch, or to a new provider;
- Assign the responsibilities of the service provider on agreement termination; and
- Potential impact on customers.

The Branch must retain the necessary expertise to supervise the outsourced functions effectively and manage the risks with the service provider and must supervise those functions and manage the risks both for the operation of the contract and during any transition/exit.

Annual review of Due Diligence

The Branch will take the necessary steps to ensure the assessment of the service provider's performance and maintain an insight on the outsourced process. This includes preventive or

corrective actions in case of relevant changes in the initial circumstances, and as part of an annual review of the service provider, their financial situation (to be made in collaboration with the Credit Department). This will be carried out by the Risk Department feeding back to the ARCo and the Branch President.

Management Oversight

Outsourcing is considered by the Branch to be an extension of the Branch's environment and is managed accordingly. The ManCo will retain overall responsibility for the control of all services that are outsourced to service providers. Day-to-day oversight of compliance with the outsourcing arrangements, and responsibility for the outsourcing policy, will be provided by the Chief Risk Officer, who will also take overarching responsibility for oversight of the outsourcing arrangements from the perspective of regulatory compliance under SYSC 8, outsourced relationships. The Head of Operations and Head of IT will offer day to day oversight of the general and IT outsourcing arrangements accordingly.

Review and sign-off

Prior to contract execution, appropriate input should be solicited from all relevant operational and business units within CNCBLB. As a minimum, the contract will have to be signed off by the President in addition to the Head of the Department responsible for the activity sought to be outsourced.

Service Level Agreements

SLAs must be put in place with all outsourced service providers, which includes both HO and third parties. The SLA will be a formally signed document where services are provided by HO and, in the case of an 'external' third party the SLA will form part of the legal contract.

In the case of outsourcing arrangements with HO, IT infrastructure and support are currently the only functions for which an SLA is necessary. However, for all new arrangements with HO it should be considered whether and SLA is necessary.

SLAs will be an important management tool for setting out clearly and upfront the scope and service level the Branch will receive and reducing the risk of non-performance or poor performance with regard to the scope, nature and quality of the services to be provided. The SLA will also set out Key Performance Indicators ("KPIs") by which the service level can be monitored. This will give the Branch a mechanism whereby it can challenge HO or a third party if the provision of service falls

below the required levels. With third parties, any disputes over the outsourcing agreement could be settled in via the appropriate legal mechanism, given the binding nature of the legally executed contract.

The contract should permit the Branch (or its internal/external auditors, and compliance officers) will have access to all books, records and information relevant to the outsourced activity, and that the outsourced service provider's performance is monitored regularly and assessed by the Branch, so that any necessary corrective measures can immediately be taken.

If appropriate, in order to avoid unacceptable business disruption, the contract should describe the contingency plans at service provider level including a plan for disaster recovery as well as periodic testing of backup facilities. It should include the frequency of these tests as well as the description of controls by the relevant department of the results of the testing.

A bilateral termination clause and minimum periods to execute a termination provision, if deemed necessary, should be included in outsourcing contracts. The latter would allow the outsourced services to be transferred to another service provider or to be reincorporated internally into the relevant Branch department. Such a clause should include provisions relating to insolvency or other material changes in the corporate form, and to intellectual property following termination, including the return of information to the Branch and other obligations, which would survive the termination of the contract.

12 Appendix B: CNCBLB Outsourcing Activity

HEAD OFFICE	System	Description	Owner	Target Availability	Target RTO	Online Service Local Time
Production network	Overseas core banking system	Engine to process customer services and transactions. It manages basic deposits and credit products, customer accounts, and payment business. The core system provides accounting support for all of Branch's banking businesses. It also provides business data for compliance, operation, risk management and financial management	Head IT	99.9%	< 2 Hours	.24/7
	Overseas counter system	Used by the counter staff (servicing wholesale customer) with a browser / server (B/S) architecture. The server is hosted in HO and the overseas branches only use terminals to access. The terminals are locally deployed and connect to HO with dedicated network lines. The counter system provides the functions of transaction display, image gathering, transaction data input (to the core system and used by other systems), and voucher printing. This system serves for corporate customers only and will be used by operation department staffs.	Head IT	99.9%	< 2 Hours	.24/7
	Parameter management system	Provides maintenance interface for accounting and business parameters	Head IT	99.9%	< 8 Hours	.24/7
	International business system	The international business system manages the business of international settlement and trade finance. It also adopts the B/S architecture with the server hosted in HO. The overseas branches use locally deployed terminals to access the server, via dedicated network lines. The international business system provides the functions of L/C, forfeiting, and trade finances.	Head IT	99.9%	< 2 Hours	.24/5
	Treasury Business system	Manages FX trade, FX options, and bonds. The front-line trading systems, including Reuters and Bloomberg, are deployed in the overseas branches. The transaction management functions, including cash management, authorisation management, and account settling, are realised by xfund system, position closing system, and cash trading system, which are deployed in HO and accessed via dedicated network lines.	Head IT	99.9%	< 2 Hours	.24/5
	xFunds trading system	FX trading and FX borrowing/lending between HO and branches (not limited in overseas branches).	Head IT	99.9%	< 2 Hours	.24/5
	Payment gateway	Provides the connectivity between the payment platform and SWIFT. It processes the payment messages.	Head IT	99.9%	< 2 Hours	.24/7
	Payment management platform	Manages the payment-related functions, including parameter maintenance, manual handlings for transaction received, process for authorisation-pending transactions, manual handlings after black-list hitting.	Head IT	99.9%	< 2 Hours	.24/7
	Exchange platform	Provides the services of message routing and transformation between different systems.	Head IT	99.9%	< 2 Hours	.24/7
	Corporate CRM system	Customer information and relationship management across the Bank.	Head IT	99.9%	< 8 Hours	.9/5 (8:30 to 17:30)
	Credit Management system	Provides credit management functions across the Bank.	Head IT	99.9%	< 8 Hours	.12/5 (8:00 to 20:00)
	Credit limit management system	Provides credit limit management functions for the "Credit management system".	Head IT	99.9%	< 8 Hours	.12/5 (8:00 to 20:00)
	Collateral management system	Provides collateral management functions for the "Credit management system".	Head IT	99.9%	< 2 Hours	.12/5 (8:00 to 20:00)
	Uniform reconciliation sysstem	Stores the customer's historical transaction data. Provides the print services of account statement, and customer notices.	Head IT	99.9%	< 2 Hours	.24/7
	Overseas AML system (black list)	Provides the filtering functions of AML black lists, which will be called during the account opening and cross-border transfers. Periodical customer information filtering will also be processed in the AML system with a batch pattern.	Head IT	99.9%	< 8 Hours	.12/5 (8:00 to 20:00)
	ODS system	The data platform of the Bank. It provides basic data for applications of HO and branches from the sources. It also cleanses the data.	Head IT	99.9%	< 2 Hours	.14/5 (8:00 to 22:00)
	Data Wharehouse	Establish the Data Warehouse infrastructure to realise the storage and process of massive data. It has high-efficient data processing ability and mix-load capability. The Data Warehouse system uses unified module policy to realise basic data consolidation and normal index processing. It provides data services for all application systems.	Head IT	99.9%	< 2 Hours	.24/7
	Domestic regulatory system	Generates statistic reports used within the Bank.	Head IT	99.9%	< 8 Hours	.12/5 (8:00 to 20:00)
	Domestic requlatory statement system	Generates reports based on the requirements from China's domestic regulators.	Head IT	99.9%	< 8 Hours	.12/5 (8:00 to 20:00)
	Overseas requlatory statement system	Generates the reports required by overseas branches and is planned to deploy in HO.	Head IT	99.9%	< 8 Hours	.12/5 (8:00 to 20:00)
	SSO uniform identification system	Provides unified account management, authentication, authorisation, and single point sign-in for the users of ODS serviced application systems.	Head IT	99.9%	< 2 Hours	.12/5 (8:00 to 20:00)
	Key Management Platform	Provides the encryption and decryption of passwords	Head IT	99.9%	< 2 Hours	.24/7
	Image content management system	Provides the storage and maintenance of business images.	Head IT	99.9%	< 2 Hours	.24/7
	OA system	The Bank's official document management system	Head IT	99.9%	< 48 Hours	.24/7
	Email system	Mail system based on Microsoft Exchange servers	Head IT	99.9%	< 48 Hours	.24/7
London branch/HO connectivity			Head IT	99.9%		.24/7
Service/Change requests			Head IT			
Service reports			Head IT			
On/Off site audits			Head IT			
Monitoring/appraisal of branch			Head IT			
DR drills for production system			Head IT			

EXTERNAL THIRD PARTIES	System	Description	Owner	Target Availability	Target RTO (HRS)
TREASURY					
Trading	Reuters	FX and Money Market news, information & trading	Head Fin Markets	Good	2
Trading	Bloomberg	Bond Market news, information & trading	Head Fin Markets	In progress	
Custodian	Clear Stream	Custodian for bonds	Head Fin Markets	In progress	
FINANCE					
Regulatory Reporting	VERMEG/Lombard Risk	PRA/FCA regulatory reporting		In progress	
Regulatory Reporting	GABRIEL	On-line UK regulatory reporting system		Good	1
Regulatory Reporting	OSCA	On-Line BOE reporting		Good	1
Tax reporting	HMRC	On-line tax reporting system		In progress	
Banking Facilities	Bank of China (Rep Office account)	Bank account /payments		Good	0
HUMAN RESOURCES					
Building Maintenance	SAVILS	99 GRESHAM Street		Good	24
Liability Insurance	China TAIPANG	Insurance cover		Good	24
Pensions	AVIVA	CNCB LB staff pension		Good	24
Medical	AVIVA	CNCB LB staff medical insurance		Good	24
Life Cover	Canada Life	CNCB LB staff life cover		Good	24
Payroll	Wilson & Co	CNCB LB payroll/ Tax		Good	2
HR Management	BREATHE	Vacation/Leave management system		Good	2
CORPORATE OFFICE					
Legal	TBA	Third-party legal services firms	President	Good	Ad-hoc
Internal Audit	BDO	Internal auditor services for CNCB LB	President	Good	
Compliance	Lexis Nexis	AML/KYC	Head of Compliance	Good	2
Telecoms	CISCO	Telephone	Head of IT	Good	2
Disaster Recovery Site	China Telecoms	CNCB LB UK DR site	Head of IT	Good	2
Committee meetings	Passageway	System to improve committee preparation	President	In progress	

13 Appendix C: Third-Party Vendor/Suppliers

TEMPLATE – EXAMPLE

Dept	Service Provider	Service description	Impact	Likelihood	Reliance rating	Owner
IT	HO	Production systems	4	1	4	D Wang
	HO	Connectivity	4	1	4	D Wang
	HO	Information Security	4	1	4	D Wang
	CISCO	Telephone	2	2	4	D Wang
	China Telcoms	DR Site	3	2	6	D Wang
FM	Reuters FX	FX trading	2	2	4	R Thaiss
	Bloomberg	Data	2	1	2	R Thaiss
	UBS	FX trading	2	2	4	R Thaiss
BD	Reuters	Data	2	2	2	Y Liu
COMP	WorldCheck	Sanctions check	4	1	4	R Sutton
RISK	Moody's	Credit Rating	3	1	3	G Lowe
	Willis Towers	D&O Insurance	3	1	3	G Lowe
	Willis Towers	Financial Crime Insurance	3	1	3	G Lowe
	Willis Towers	Cyber Insurance	3	1	3	G Lowe
HR	Savills	Building maintenance	3	2	6	M Boyce
	AVIVA	Pensions/Health cover	3	1	3	M Boyce
	Canada Life	Life Cover	4	1	4	M Boyce
	China Taipang	Liability insurance	4	1	4	M Boyce
FINCON	Lombard Risk	Regulatory reporting	4	2	8	C Marshall

Reliance rating - the reliance factor reflects the importance to CNCBLB business requirements. This rating will require assessment of both:

- Impact assessment must consider strategic fit, volumes, value, controls, monitoring and reporting capabilities, financial and regulatory implications
- Likelihood assessment must consider complexity, contractual obligations covering the level of support, the service provided and if alternate to the service is available

Risk department will maintain list of suppliers and risk register and will initiate reviews and risk assessments, at least annually. The ManCo will determine actions required for High Risk suppliers/vendors, including:

- Additional actions that could be taken;
  - Contact review;
  - Performance review;
  - Financial/Credit review;
  - Access to premises; and
  - Contingency and Disaster Recovering plan review.
- Link to Department RCSA's and/or any Internal Audit findings.

Methodology

Supplier/vendor risk calculated using the R= I X L formula where the risk is assessed using the following risk table:

IMPACT	
Critical	4
High	3
Medium	2
Low	1

LIKELIHOOD	
No support, high vulnerability to an event	4
Supported with unknown service level	3
Supported with adequate service level	2
Strong support with good service level	1

High	10 ➔ 16
Medium	4 ➔ 9
Low	1 ➔ 3

14 Appendix D: Outsourcing Agreement Checklist

As contract law can be complicated, CNCBLB owners of outsourcing relationships need to ensure the branch is always protected. In most cases, external legal advice should be taken for any significant outsourcing arrangements. The checklist below provides some guidance to potential risks when considering outsource contracts, MOU's or Service Level Agreements:**Parties**	- Contracting parties, legal structure, authority and jurisdictions - Third party beneficiaries, e.g. affiliates, customers - Agents and subcontractors - Guarantees from the customer/vendor's parent company - Required consents
Transitional Provisions (Commencement and Transitioning-in)	- Allocation of responsibility for orderly and efficient transition - Employee transfers, if required - Timetable - Consequences of Delay - Commencement of service levels
Services and Change Orders	- Scope of services • Due diligence on scope • Risk of undisclosed services • Exclusivity of right of first refusal clauses - Clear change order process • Triggers, e.g. by either party, government, regulatory environment, force majeure • Change management • Requests and responses • Acceptance, rejection and reviews • Pricing parameters for additional services • Tie into governance • Exclusions - Service levels and Remedies • When will service levels start? Concurrent with warranties? During testing, initial phases, rollout? • Initial grace period • How are service levels being set/measured? Cost, timing. Outcomes, results, surveys, quantitative and qualitative criteria • Service level guarantees vs. objectives/targets • Weighting of services performed • Reference to existing, third party, or industry standard service levels and specifications • Verification of performance • Periodic reports • Internal of third party audits • End user surveys, stakeholder reviews - Failures, termination, relief, remedies(e.g. credits,

	refunds, discounts, repricing changes to scope/services, phase-out, business continuity and disaster recovery plan initiation, termination, repatriation, etc.)
Subcontracting	- Approval, review process - Pre-existing, pre-approved list - Liability for third parties, default, remedies, indemnities - Control, limitations - Insurance - Audit - Warranties, liens, waivers - Assignment
Pricing	- Base price (Fixed or Variable) - Pass-through expenses and/or service level credits - Inflation adjustments, cost of living adjustments(COLA) - Measurement methodology, reporting, audit - Innovation, improvements, cost saving and gain sharing - Most favoured customer - Invoicing, payment, timing, currency - Late charges, prepayments, refunds - Taxes, credits
Benchmarking	- Quality of service, results, outcomes - Price benchmarking: comparison against other organizations that are outsourced - Cost benchmarking: comparison against insourced organizations - Benchmarking provisions: • Frequency: daily, weekly, monthly, yearly? • Subgroups: Which services will be measured? • Costs: how will benchmarking be paid for? • Focus: cost, quality or both?
Intellectual Property Rights	- Ownership of intellectual property (during and post term of agreement) - Assignments and transfers of ownership - Licenses • Patents, Trademarks, Copyrights • Scope of rights, e.g. make, use, copy, sell, distribute, etc. • Term and termination, survival • Transferability and change of control impact • Exclusive vs. non-exclusive • Indemnities for infringement
Security, Privacy and Confidentiality	- Compliance with corporate policies - Criminal, financial premises, systems checks - Privacy laws and regulatory guidelines - Responsibility for third party compliance – cannot contract out of accountability - Scope of confidential information and trade secrets - Inclusions/ Exclusions, access, permitted disclosure - Timing, term of agreement - Return and destruction - Notification and remedies for breach / Indemnities
Limitation of Liability	- Exclusions, e.g. for indirects, special, consequential, privacy/security breaches - Lost profits (could be direct or indirect) - Types of damages included

	- Claims by beneficiaries of services or third parties - Liability for assignees and subcontractors - Limitation periods
Warranties	- Corporate and organizational - Authority - Litigation and consents - Quality, systems, service levels, performance - Subcontractors and third parties
Indemnities	- Beneficiaries - Scope, e.g. only third party claims, territory - Actions required by indemnitor, e.g. defend, modify, replace non-infringing software - Actions required by indemnitee, e.g. notify and implement changes right to step in and defend litigation - Insurance to ensure indemnitor has sufficient financial backing
Business Continuity Planning	- Requirements for disaster recovery plan - Testing - Loss or theft of data - Data backup storage - Media and communications management in case of disaster - Scope of force majeure clauses
Dispute Resolution	- Resolution prior to litigation - Escalation levels for grievances - Alternative dispute resolution mechanisms
International agreements	- Choice of law - Choice of jurisdiction, dispute resolution - Currency - Language - Withholding taxes - Local regulations, e.g. employment, outsourcing guidelines/regulations
Termination and Transition	- Term of agreement, various services and extension options - Vendor/Customer termination provisions - Cause (Convenience, Change of control, Insolvency, Force Majeure) - Notice periods - Termination fees
Transition Issues	- Cooperation, knowledge transfer and the provision of assistance in transfer activities - Assignment of licenses and agreements - Solicitation of key employees, announcements, responsibility benefits - Division of costs associated with transition - Privacy and confidentially